



ASA-1157

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:

	K. SHIGA et al.	Confirmation No.: 4267
Serial No.	10/664,891	Group Art Unit: 2157
Filed:	September 22, 2003	Examiner: A.E. Salad
For:	STORAGE NETWORK MANAGEMENT SYSTEM AND METHOD	
Customer No.:	24956	

**SUBMISSION OF CERTIFIED PRIORITY DOCUMENT**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

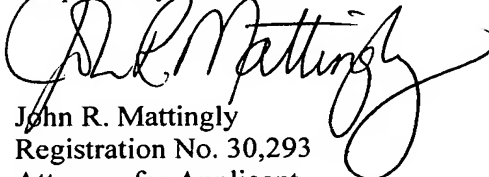
Sir:

Applicants submit herewith a certified priority document of the corresponding Japanese Patent Application:

No. 2003-206165, filed August 6, 2003, for the purpose of claiming foreign priority under 35 U.S.C. § 119.

Applicants respectfully request that the priority document be submitted and officially considered of record.

Respectfully submitted,

  
John R. Mattingly  
Registration No. 30,293  
Attorney for Applicant

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.  
1800 Diagonal Road, Suite 370  
Alexandria, Virginia 22314  
(703) 684-1120  
Date: July 5, 2006

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

CERTIFIED COPY OF  
PRIORITY DOCUMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日      2 0 0 3 年   8 月   6 日  
Date of Application:

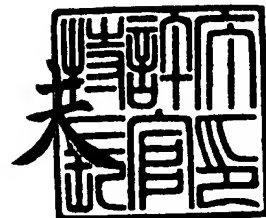
出 願 番 号      特 願 2 0 0 3 - 2 0 6 1 6 5  
Application Number:  
[ST. 10/C]:      [ J P 2 0 0 3 - 2 0 6 1 6 5 ]

出   願   人      株 式 会 社 日 立 製 作 所  
Applicant(s):

2 0 0 3 年 1 0 月 2 8 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号    出証特 2 0 0 3 - 3 0 8 8 7 8 1

【書類名】 特許願

【整理番号】 K03009071A

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/44

【発明者】

    【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

    【氏名】 志賀 賢太

【発明者】

    【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

    【氏名】 熊谷 敦也

【発明者】

    【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

    【氏名】 藤原 啓成

【特許出願人】

    【識別番号】 000005108

    【氏名又は名称】 株式会社 日立製作所

【代理人】

    【識別番号】 100075096

    【弁理士】

    【氏名又は名称】 作田 康夫

【手数料の表示】

    【予納台帳番号】 013088

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

【物件名】 要約書 1  
【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ストレージネットワーク管理装置及び方法

【特許請求の範囲】

【請求項 1】

計算機、ストレージ装置及びスイッチを有するストレージネットワークを管理する管理装置であって、

制御部、前記スイッチと接続されるインターフェース及び管理者が使用する入力インターフェースを有し、

前記スイッチに前記計算機又は前記ストレージ装置が接続された場合、

前記インターフェースを介して前記スイッチに接続された前記計算機又は前記ストレージ装置から得られる前記計算機又は前記ストレージ装置の第一の識別子の情報及び第二の識別子の情報、前記インターフェースを介して前記スイッチから得られる前記スイッチに接続される前記計算機又は前記ストレージ装置の前記第二の識別子と前記計算機又は前記ストレージ装置が接続される前記スイッチのインターフェースを識別する第三の識別子との対応関係の情報、並びに前記入力インターフェースを介して前記管理者が入力した所定のグループを構成する前記計算機又は前記ストレージ装置を識別するための前記第一の識別子に関する情報に基づいて、前記所定のグループに属する前記スイッチの前記第三の識別子を特定し、

前記入力インターフェースから前記ストレージ装置が有する記憶領域と前記記憶領域を使用可能な前記計算機を示す前記第一の識別子に関する情報が入力された場合、前記ストレージ装置に前記入力された情報を送信してセキュリティの設定を指示するとともに、前記第一の識別子に対応する前記スイッチの前記第三の識別子及び前記第三の識別子が属する前記グループの情報を抽出し、前記スイッチに前記抽出した情報を送信して前記グループに対応する仮想 LAN の設定を指示することを特徴とする管理装置。

【請求項 2】

前記第一の識別子はインターネットプロトコル（IP）アドレス、前記第二の識別子は MAC アドレス、前記第三の識別子はポート ID、前記第一の識別子に

関する情報とはサブネットアドレスであることを特徴とする請求項 1 記載の管理装置。

【請求項 3】

前記 MAC アドレスを前記計算機に ARP コマンドを送信することによって取得し、前記 MAC アドレスと前記ポート ID との対応関係を前記スイッチから SNMP の Get コマンドを用いて取得することを特徴とする請求項 2 記載の管理装置。

【請求項 4】

前記スイッチに接続された前記計算機から SLP のパケットを受信することで、前記計算機が前記スイッチに接続されたことを検出することを特徴とする請求項 3 記載の管理装置。

【請求項 5】

前記スイッチへ指示される内容とは、前記第三の識別子を、前記グループに対応する仮想 LAN に追加する指示であることを特徴とする請求項 1 記載の管理装置。

【請求項 6】

前記グループに対応する仮想 LAN が前記スイッチで設定されていない場合には、前記指示は、前記グループに対応する仮想 LAN を新たに生成する指示であることを特徴とする請求項 5 記載の管理装置。

【請求項 7】

前記スイッチから前記計算機又は前記ストレージ装置が取り外された場合、前記取り外された前記計算機又は前記ストレージ装置が属する前記グループに対応する仮想 LAN から前記取り外された前記計算機又は前記ストレージ装置に対応する前記第三の識別子を削除するよう前記スイッチに指示することを特徴とする請求項 6 記載の管理装置。

【請求項 8】

前記取り外された前記計算機又は前記ストレージ装置に対応する前記第三の識別子を前記グループに対応する前記仮想 LAN から削除することによって前記グループに所属する前記計算機又は前記ストレージ装置がなくなってしまった場合

、前記スイッチに前記仮想 LAN 自体を削除する指示を行うことを特徴とする請求項 7 記載の管理装置。

【請求項 9】

計算機とストレージ装置に接続されるスイッチであって、

制御部、前記ストレージ装置又は前記計算機と接続されるインターフェース及び管理者が使用する入力インターフェースを有し、

前記インターフェースに前記計算機又は前記ストレージ装置が接続された場合

、  
前記制御部は、前記インターフェースを介して前記接続された前記計算機又は前記ストレージ装置から得られる前記計算機又は前記ストレージ装置の第一の識別子の情報及び第二の識別子の情報、該スイッチが有する該スイッチに接続される前記計算機又は前記ストレージ装置の前記第二の識別子と前記計算機又は前記ストレージ装置と接続される該スイッチのインターフェースを識別する第三の識別子との対応関係の情報、並びに前記入力インターフェースを介して前記管理者が入力した所定のグループを構成する前記計算機又は前記ストレージ装置を識別するための、前記第一の識別子に関する情報に基づいて、前記所定のグループに属する前記計算機又は前記ストレージ装置に対応する前記第三の識別子を特定し

、  
前記入力インターフェースから前記ストレージ装置が有する記憶領域と前記記憶領域を使用可能な前記計算機を示す前記第一の識別子に関する情報が入力された場合、前記ストレージ装置に前記入力された情報を送信してセキュリティの設定を指示するとともに、前記第一の識別子に対応する前記第三の識別子及び前記第三の識別子が属する前記グループの情報を抽出し、前記グループに対応する仮想 LAN の設定を行うことを特徴とするスイッチ。

【請求項 10】

計算機に接続されるスイッチと接続されるストレージ装置であって、

制御部、前記スイッチと接続されるインターフェース、管理者が使用する入力インターフェース及び記憶領域を有し、

前記スイッチに前記計算機が接続された場合、

前記インターフェースを介して前記接続された前記計算機から得られる前記計算機の第一の識別子の情報及び第二の識別子の情報、前記インターフェースを介して前記スイッチから得られる前記スイッチに接続される前記計算機の前記第二の識別子と前記計算機と接続される前記スイッチのインターフェースを識別する第三の識別子との対応関係の情報、並びに前記入力インターフェースを介して前記管理者が入力した所定のグループを構成する前記計算機を識別するための、前記第一の識別子に関する情報に基づいて、前記所定のグループに属する前記計算機に対応する前記第三の識別子を特定し、

前記入力インターフェースから前記記憶領域と前記記憶領域を使用可能な前記計算機を示す前記第一の識別子に関する情報が入力された場合、セキュリティの設定をするとともに、前記第一の識別子に対応する前記第三の識別子及び前記第三の識別子が属する前記グループの情報を抽出し、前記グループに対応する仮想 LAN の設定を前記スイッチに指示することを特徴とするストレージ装置。

【請求項 11】

計算機、ストレージ装置及びスイッチを有するストレージネットワークを管理する管理方法であって、

前記スイッチに前記計算機又は前記ストレージ装置が接続された場合、

前記接続された前記計算機又は前記ストレージ装置から得られる前記計算機又は前記ストレージ装置の第一の識別子の情報及び第二の識別子の情報、前記スイッチから得られる前記スイッチに接続される前記計算機又は前記ストレージ装置の前記第二の識別子と前記計算機又は前記ストレージ装置と接続される前記スイッチのインターフェースを識別する第三の識別子との対応関係の情報、並びに所定のグループを構成する前記計算機及び前記ストレージ装置を識別するための、前記第一の識別子に関する情報に基づいて、前記所定のグループに属する前記計算機又は前記ストレージ装置に対応する前記第三の識別子を特定し、

前記ストレージ装置が有する記憶領域と前記記憶領域を使用可能な前記計算機を示す前記第一の識別子に関する情報を基に、前記ストレージ装置でセキュリティの設定をするとともに、前記第一の識別子に対応する前記第三の識別子及び前記第三の識別子が属する前記グループの情報を抽出し、前記スイッチで前記グル



ープに対応する仮想LANを設定することを特徴とする管理方法。

【請求項12】

ストレージ装置、スイッチ及び計算機がネットワークで接続されているストレージシステムの管理方法であって、

前記ストレージ装置の記憶領域の識別子と前記計算機の第一のアドレスに基づき、前記記憶領域の識別子に対するアクセス制御設定を前記ストレージ装置に対して実行し、前記計算機の第一のアドレスを第二のアドレスに変換し、前記計算機の前記第二のアドレスを前記計算機が接続している前記スイッチのポートの識別子に変換し、前記ポートの識別子を仮想LANに追加する設定を前記スイッチに対して実行することを特徴とする方法。

【請求項13】

ストレージ装置、スイッチ及び計算機がネットワークで接続されているストレージシステムの管理方法であって、

前記ストレージ装置の記憶領域の識別子と計算機の第一のアドレスに基づき、前記記憶領域に対する前記計算機のアクセス制御設定を前記ストレージ装置で実行し、

前記計算機の第一のアドレスを第二のアドレスに変換し、前記計算機の第二のアドレスを計算機が接続している前記スイッチのポートの識別子に変換し、前記ポートをVLANに追加する設定を前記スイッチに対して実行することを特徴とする管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークに接続されたストレージ装置と複数の情報処理装置から構成されるシステムに関する。

【0002】

【従来の技術】

近年、ファイバチャネル（以下「FC」）のネットワークよりも導入コストが低いIPネットワークを用いたネットワークストレージ技術であるIP-SAN

が注目を集めている。しかし、IPネットワークは、セキュリティ上の脅威を与えるクラッキングツールが多く出回る等、セキュリティの確保にコストが掛かる。

#### 【0003】

従来のFC-SANにおけるセキュリティ対策としては、LUN (Logical Unit Number) マスキングが実施されていた。LUNマスキングとは、ストレージ装置が有する論理ボリューム (Logical Unit。以下、LUと略す) にアクセス可能な計算機をストレージ装置側で制限することで、不正なデータの参照、改ざん、及び消去などを防止する技術である。

#### 【0004】

FC-SANのLUNマスキング技術をIP-SANで実現する場合、ストレージ装置が有するLUごとに、当該LUにアクセス可能な計算機をその計算機に割り振られたIPアドレスで指定する。しかし、IPネットワークでは同じサブネットに接続された他の計算機が送受信するパケットの盗聴が容易である。したがって、同一のネットワークを二つ以上の部署や業務の計算機が共用している場合、データの機密性が確保できず、LUNマスキングの設定だけでは十分なセキュリティ対策にならない。したがって、他のセキュリティ技術との併用を考えなければならない。

#### 【0005】

併用するセキュリティ技術の候補として、IPSecなどの技術を用いたデータの暗号化が挙げられる。しかし、暗号化処理はCPUへの負荷が高い処理であり、これをIP-SANに適用すると、ストレージ装置に対するI/O性能が劣化してしまう。このような性能劣化を改善するために、暗号化処理を専用ハードウェアで実行させてもよいが、導入コストが高くなるので、併用するセキュリティ技術としては採用しがたい。

#### 【0006】

他のセキュリティ技術の候補として、一つの物理的なネットワークを複数の論理的なネットワークに分割するVLAN (Virtual Local Area Network) という技術が挙げられる。本技術では、同じ部署が使用す

る計算機など、データ盗聴が問題にならない一つ以上の計算機をグループ化し、そのグループごとにネットワークを論理的に分割することで、グループ間のデータ盗聴を防止することができる。しかも、VLANは、ほとんどのLANスイッチで採用されている技術であり、追加の導入コストが発生することもない。従って、IP-SANのセキュリティ対策は、LUNマスキングとVLANの技術を併用することが多くなると考えられる。

#### 【0007】

又、VLANの設定作業の負荷を軽減する技術が、特許文献1に開示されている。

#### 【0008】

##### 【特許文献1】

特開 2001-53776 号公報

#### 【0009】

##### 【発明が解決しようとする課題】

しかし、LUNマスキングの設定作業はストレージ装置で行う一方で、VLANの設定作業はIP-SAN内のスイッチに対して行う必要がある。このように、異なる装置に対して設定作業を実施する必要があるため、システムの利用者又は管理者の作業負荷が大きい。

#### 【0010】

さらに、LUNマスキングの設定作業では、計算機をIPアドレス（或いはドメイン名）で指定するのに対して、VLANの設定作業では、計算機を接続先スイッチのポートを識別するポートIDで指定する必要がある。このように、LUNマスキングとVLANの設定作業は、計算機を異なる識別子で指定しなければならないため、設定ミスが発生し易い。

#### 【0011】

更に、特許文献1に開示された技術は、計算機の接続先スイッチを変更した時のVLANの設定作業を自動化するものであって、上記のような問題を解決することはできない。

#### 【0012】

本発明の目的は、VLAN及びLUNマスキングの設定を容易に行えるシステムを提供することである。

#### 【0013】

##### 【課題を解決するための手段】

本発明の一実施形態は、以下の通りである。

ストレージ装置、スイッチ及び計算機がネットワークで接続されているストレージシステムの管理方法として、ストレージ装置の記憶領域の識別子と計算機の第一のアドレスに基づき、記憶領域に対する計算機のアクセス制御設定をストレージ装置に対して実行し、計算機の第一のアドレスを第二のアドレスに変換し、計算機の第二のアドレスを計算機が接続しているスイッチのポートの識別子に変換し、そのポートをVLANに追加する設定を前記スイッチに対して実行するステップを有する構成とする。

#### 【0014】

上述の実施形態では、システム管理者が、LUNマスキング設定と共に、グループを構成する計算機やストレージ装置が属するVLANのサブネットアドレスの入力を行うと、計算機やストレージ装置がネットワークに接続された時に、ストレージ管理装置が、自動的にVLANの設定を行う構成を有する。

#### 【0015】

尚、上述した方法は、ストレージ管理装置で実行されても、スイッチで実行されても、ストレージ装置で実行されても良い。

#### 【0016】

##### 【発明の実施の形態】

以下、本発明の実施形態について図面を用いて説明する。以下の図中、同一の部分には同一の符号を付加する。

#### 【0017】

最初に、本発明を適用した計算機システムの第一の実施形態を説明する。第一の実施形態では、IP-SANセキュリティ管理を、ストレージ装置の構成管理や監視を行うストレージ管理装置で実施する。

#### 【0018】

図1は、第一の実施形態の構成例を示した図である。計算機システムは、ストレージ管理装置1、ストレージ装置2、パケットを転送するスイッチ3及びホスト4を有し、各構成要素が通信線20aを介して相互に接続されている。

#### 【0019】

ストレージ装置2は、単体の記憶装置又は複数の記憶装置を有する記憶装置システムである。尚、記憶装置には、ハードディスクドライブやDVDと言った、不揮発性の記憶媒体を用いた装置等が含まれる。又、記憶装置システムでは、RAID構成が採用されていても良い。ストレージ装置2は、スイッチ3やホスト4と通信線20aを介して接続するための物理的なポート（以下「物理ポート」）41を有する。

ホスト4は一般的な計算機であり、演算部、メモリ、入出力部等を有する。又、ホスト4は、他の装置と通信線20aを介して接続するための物理ポートを有する。

#### 【0020】

スイッチ3は、ホスト4やストレージ装置2から転送されるデータを他の装置に転送する装置である。スイッチ3は、ストレージ装置2と接続するための物理ポート42及びホスト4又は他のスイッチ3と接続するための物理ポート43を有する。尚、物理ポート42と43を物理的に区別する必要は無いが、以下の説明の便宜上、区別しておく。

#### 【0021】

さらに、ストレージ管理装置1、ストレージ装置2及びスイッチ3は、監視や保守用のデータが流れる通信線20bによっても相互に接続されているものとする。なお、通信線20bを使用せず、監視や保守用データも通信線20aを介して相互に授受されてもよい。さらに、本実施形態では、スイッチ3が2台、ホスト4が4台の構成の場合について説明するが、本発明はスイッチやホストの台数が何台であっても問題ない。

#### 【0022】

尚、ストレージ装置2はiSCSIターゲットになることができる。又、ストレージ装置2は制御部を有し、制御部は、LUNマスキングに関する設定情報を

ストレージ装置 2 の外部から受信し LUN マスキングを設定する。

#### 【0023】

一方、スイッチ 3 は、制御部を有し、制御部は、VLAN に関わる設定情報をスイッチ 3 の外部から受信し VLAN 設定を実行する。又、スイッチ 3 の制御部は、外部装置の要求に応じてフォワーディングデータベースを送信したり、リンクダウンを外部装置に通知する。

#### 【0024】

ストレージ管理装置 1 は、一般的な計算機であり、中央演算装置（以下「CPU」という）24、ハードディスク等の 2 次記憶装置（以下「磁気ディスク」という）23、主記憶装置メモリ（以下「主メモリ」という）21、バスやクロスバススイッチなどの通信線 22、表示装置などの出力装置（以下「ディスプレイ」という）25、キーボードなどの文字入力装置 27 及びマウスなどのポインティング装置 26 を有する。更に、ストレージ管理装置 1 は、通信線 20a 及び 20b と接続するためのインターフェースも有する。

#### 【0025】

主メモリ 21 には、CPU 24 が実行する各種プログラムが格納される。具体的には、システム管理者にグラフィカルなユーザインターフェースを提供する際に CPU 24 で実行される GUI 制御プログラム 10、iSCSI ターゲットからの登録を受信したり iSCSI イニシエータ（ホスト）からの iSCSI ターゲットのディスカバリ要求を受信し応答を返す際に実行されるディスカバリ要求受信プログラム 11、ARP（Address Resolution Protocol、RFC 826）を用いて、ストレージ管理装置 1 が IP アドレスと MAC アドレスとの間の変換を行う際に実行される ARP 送信プログラム 12、スイッチ 3 からフォワーディングデータベースを取り出し、MAC アドレスを物理ポートの識別子であるポート ID に変換する際に実行されるポート ID 取得プログラム 13、ストレージ装置 2 に対して LUN マスキングの設定をする際に実行される LUN マスキング設定プログラム 14 及びスイッチ 3 に対して VLAN の設定をする際に実行される VLAN 設定プログラム 15 である。

#### 【0026】

ここで、フォワーディングデータベースとは、スイッチ3が有する、ポートIDとそのポートIDで示される物理ポート42（又は43）と接続される装置のMACアドレスとの対応関係を示す表である。又、IPアドレスとは、通信線20のプロトコルにインターネットプロトコルを使用する際に、各装置に割り当てられる識別子である。更に、MACアドレスとは、各装置に割り当てられている固有の識別子である。

#### 【0027】

又、iSCSIイニシエータとは、iSCSIコマンドを主体的に発行する装置で、本実施形態ではホスト4に該当する。又、iSCSIターゲットとは、iSCSIイニシエータが通信の相手とする装置であり、本実施形態では、ストレージ装置2、又はその中に含まれるLU等が該当する。

#### 【0028】

尚、上述のプログラムは、あらかじめ、または可搬型記録媒体からの読み込み、または他の計算機からのネットワーク経由のダウンロードにより、磁気ディスク23に格納される。これらのプログラムは、必要に応じて主メモリ21に転送され、CPU24で実行される。なお、これらのプログラムが専用のハードウェアとして実装されていても良い。

#### 【0029】

磁気ディスク23には、ホスト4やストレージ装置2の物理ポートに対応するIPアドレス、MACアドレス及び当該物理ポートと接続されているスイッチ側の物理ポートのポートIDとの対応関係を記憶するアドレステーブル30、iSCSIイニシエータとiSCSIターゲット（これらをあわせて「iSCSIノード」という）から構成されるグループのIDと、そのグループが属するVLANのサブネットアドレスを記憶するグループテーブル31、グループを構成するiSCSIイニシエータのIPアドレスとiSCSIターゲットのiSCSI名前を記憶するグループメンバーテーブル32、iSCSIターゲットとそれに含まれるLUごとにアクセス可能なiSCSIイニシエータのIPアドレスを記憶するLUNマスキングテーブル33、iSCSIターゲットの名前とIPアドレスの対応関係を記憶するiSCSI名前テーブル34及びスイッチの管理用物

理ポートのIPアドレスを記憶するスイッチテーブル35を格納する。

#### 【0030】

尚、上述のグループは、同じ部署や業務で利用されるホスト4など、セキュリティ上、データの盗聴が問題とならない一つ以上のiSCSIイニシエータとそれらが使用するiSCSIターゲットから構成されるものとする。

#### 【0031】

ここで、第一の実施形態のストレージ管理装置1の動作を簡単に説明する。まず、システム管理者は、計算機システム内に設置されたスイッチ3をスイッチテーブル35に登録しておく。次に、システム管理者はグループをグループテーブル31に登録する。その後、ストレージ装置2がスイッチに接続されると、ストレージ管理装置1が接続されたストレージ装置2が属するグループを判定し、そのストレージ装置2をグループのメンバに追加すると共に、そのグループに対応するVLANにそのストレージ装置2を追加するようスイッチ3に指示する。

#### 【0032】

次に、システム管理者がLUNマスキングの設定を行うと、ストレージ管理装置1が、ストレージ装置2に対してLUNマスキングの設定を指示するとともに、LUNマスキングで指定したホスト4のグループを判定し、そのホスト4をグループのメンバに追加する。その後、そのホスト4がスイッチ3に接続されると、ストレージ管理装置1が、そのホスト4が属するグループのVLANにそのホスト4を追加するようスイッチ3に指示する。次にストレージ管理装置1の磁気ディスク23に格納された各種テーブルのデータ構造について説明する。

アドレステーブル30、グループテーブル31、グループメンバテーブル32、LUNマスキングテーブル33、iSCSIネームテーブル34及びスイッチテーブル35は、配列構造を成し、1以上のレコードを格納可能である。

#### 【0033】

図2(a)は、アドレステーブル30のデータ構造例を示す図である。アドレステーブル30は、ホスト4又はストレージ装置2が有する物理ポート毎に一つのレコードを有する。個々のレコードは、レコードに対応する物理ポートに割り振られたIPアドレスが登録されるエントリ300、レコードに対応する物理ポ



ートに割り振られたMACアドレスが登録されるエントリ301、レコードに対応する物理ポートが接続されているスイッチ3の識別子であるスイッチIDが登録されるエントリ302及びレコードに対応する物理ポートが接続されているスイッチ側の物理ポートのポートIDが登録されるエントリ303を有する。

#### 【0034】

図2(b)は、グループテーブル31のデータ構造例を示す図である。グループテーブル31は、グループ毎に対応するレコードを有する。グループテーブル31の各レコードは、レコードに対応するグループの識別子であるグループIDが登録されるエントリ310、レコードに対応するグループを構成するiSCSIイニシエータ及びiSCSIターゲットが所属するVLANのサブネットアドレスが登録されるエントリ311を有する。尚、本実施形態では、グループIDはVLAN IDとしても使用されるため、1から4096までの整数値をとるものとする。

#### 【0035】

図2(c)は、グループメンバーテーブル32のデータ構造例を示す図である。グループメンバーテーブル32は、iSCSIノードごとに対応するレコードを有する。各レコードは、レコードに対応するiSCSIノードが属するグループのグループIDが登録されるエントリ320、レコードに対応するiSCSIノードのIPアドレスが登録されるエントリ321、レコードに対応するiSCSIノードがiSCSIイニシエータかiSCSIターゲットかを区別する情報が登録されるエントリ322及びレコードに対応するiSCSIノードが通信線20aに接続されているか否かを表す接続フラグの情報が登録されるエントリ323を有する。

#### 【0036】

尚、本実施形態では、エントリ322に登録される情報は「イニシエータ」か「ターゲット」のどちらかをとるものとする。又、エントリ323は、レコードに対応するiSCSIノードが通信線20aに接続されている場合「1」、接続されていない場合「0」の情報が登録されるものとする。

#### 【0037】

図3 (a) は、LUNマスキングテーブル33のデータ構造例を示す図である。LUNマスキングテーブル33は、iSCSIターゲットに付与されたiSCSIネーム毎に対応するレコードを有する。各レコードは、レコードに対応するiSCSIネームを記憶するエントリ330、レコードに対応するiSCSIネームで指定されるiSCSIターゲットに含まれるLUのLUNが登録されるエントリ331及びエントリ331に登録されたLUにアクセス可能なiSCSIイニシエータのIPアドレスが登録されるエントリ332を有する。

#### 【0038】

図3 (b) は、iSCSIネームテーブル34のデータ構造例を示す図である。iSCSIネームテーブル34は、iSCSIターゲットに付与されたiSCSIネーム毎に対応するレコードを有する。各レコードは、レコードに対応するiSCSIネームが登録されるエントリ340、レコードに対応するiSCSIネームで指定されるiSCSIターゲットのIPアドレスが登録されるエントリ341及びレコードに対応するiSCSIネームで指定されるiSCSIターゲットに対応するポート番号が登録されるエントリ342を有する。

#### 【0039】

図3 (c) は、スイッチテーブル35のデータ構造例を示す図である。スイッチテーブル35は、システムに含まれるスイッチ3ごとに对应するレコードを有する。各レコードは、レコードに対応するスイッチ3を指定するスイッチIDが登録されるエントリ350及びレコードに対応するスイッチの管理用物理ポートに割り当てられたIPアドレスである管理用IPアドレスが登録されるエントリ351を有する。

#### 【0040】

次に、本実施形態で用いられるグラフィカルユーザインタフェース（以下「GUI」）について説明する。これらのGUIは、ストレージ管理装置1がGUI制御プログラム10を実行することによってディスプレイ25に表示される。システム管理者等は、文字入力装置27及びポインティング装置26を用いて各パラメータを表示されたGUI上で設定する。

#### 【0041】

なお、ディスプレイ 25、文字入力装置 27 及びポインティング装置 26 は、ストレージ管理装置 1 と別装置であっても良い。例えば、ストレージ管理装置 1 と通信線 20b 或いはシリアルケーブルを介して接続されるコンソール用端末がディスプレイ 25 等を有していても良い。この場合、ストレージ管理装置 1 は、GUI 制御プログラム 10 を実行して画面データをコンソール用端末へ送信し、コンソール用端末がディスプレイ 25 に GUI を表示する。

#### 【0042】

さらに、コンソール用端末は、システム管理者等が文字入力装置 27、ポインティング装置 26 を用いて設定した各パラメータをストレージ管理装置 1 へ送信する。なお、ストレージ管理装置 1 は、本実施形態で説明する GUI のかわりに、その GUI と同等の機能を有するコマンドラインインターフェースを備えてもよい。

#### 【0043】

図 4 (a) は、システム管理者が LUN マスキング設定を行うために使用する LUN マスキング設定画面 400 の表示例を示す図である。LUN マスキング設定画面 400 は、iSCSI ターゲットの iSCSI ネームを選択するボタン 401、ボタン 401 で選択された iSCSI ネームを表示する領域 402、iSCSI ターゲット内の LUN を選択するボタン 403、ボタン 403 で選択された LUN を表示する領域 404、iSCSI イニシエータの IP アドレスを入力する領域 405、これらの領域やボタンで指定された情報を登録する際に指定されるボタン 406、及び登録を取り消す際に指定されるボタン 407 を有する。

#### 【0044】

以下、GUI 操作で LUN マスキングが設定される時のストレージ管理装置 1 の処理について説明する。尚、以下の処理は、GUI 操作プログラム 10 の実行によって行われる。

システム管理者等がポインティングデバイス等を用いてボタン 406 を押下すると、ストレージ管理装置 1 は、領域 402、領域 404 及び領域 405 に表示された内容に基づき、LUN マスキングテーブル 33 に新規レコードを追加する。

次にストレージ管理装置 1 は、グループテーブル 31 の各レコードについて、領域 405 に入力された IP アドレスがエントリ 311 に登録されたサブネットアドレスに属するか調べ、サブネットに属する場合、グループメンバテーブル 32 にレコードを追加する。ここで、追加されるレコードのエントリ 320 にはグループテーブル 31 の当該レコードのエントリ 310 のグループ ID、エントリ 321 には領域 405 の内容、エントリ 322 には「イニシエータ」、エントリ 323 には「0」が各々登録される。

#### 【0045】

領域 405 に入力された IP アドレスがグループテーブル 31 のあるレコードのサブネットに属する場合は、ストレージ管理装置 1 はさらに、領域 402 に入力された iSCSI ネームを持つ iSCSI ターゲットがグループメンバテーブル 32 に登録されているか調べ、未登録であれば、グループメンバテーブル 32 にレコードを追加する。この場合、追加されるレコードのエントリ 320 にはグループテーブル 31 の当該レコードのエントリ 310 のグループ ID、エントリ 321 には領域 401 の内容、エントリ 322 には「ターゲット」、エントリ 323 には「0」が各々登録される。

#### 【0046】

最後に、ストレージ管理装置 1 は、LUN マスキング設定プログラム 14 を実行して、ストレージ装置 2 に対して LUN マスキングの設定を指示する。具体的には、ストレージ管理装置 1 は、LUN マスキングテーブル 33 に登録された情報をストレージ装置 2 へ送信し、送信された情報に基づいて LUN マスキングを設定、具体的には、指定された IP アドレスで指定されるホスト 4 から、指定された iSCSI ネームのターゲットへのアクセスを許可する設定をするように、ストレージ装置 2 の制御部へ指示を送る。

#### 【0047】

図 4 (b) は、システム管理者が、グループを登録するために使用するグループ登録画面 420 の表示例を示す図である。グループ登録画面 420 は、システム管理者が新規グループ ID の入力を行う領域 421、グループを構成する iSCSI ノードが所属する VLAN のサブネットアドレスを入力する領域 422、

これらの領域やボタンで指定された情報を登録する際に指定されるボタン 423、及び登録を取り消す際に指定されるボタン 424 を有する。

#### 【0048】

以下、GUI 操作により、グループが登録される際のストレージ管理装置 1 の処理について説明する。尚、本処理も、ストレージ管理装置 1 が GUI 制御プログラム 10 を実行することで行われる。

システム管理者等がグループ登録画面 420 のボタン 423 をポインティングデバイス等で指定すると、ストレージ管理装置 1 はまず、グループテーブル 31 にレコードを追加する。追加されるレコードのエントリ 310 には領域 421 の内容、エントリ 311 には領域 422 の内容が登録される。

#### 【0049】

次にストレージ管理装置 1 は、LUN マスキングテーブル 33 から、領域 422 のサブネットに属する IP アドレスを持つレコードを選択する。そして、ストレージ管理装置 1 は、選択されたレコードの情報に従って、iSCSI イニシエータのレコードと iSCSI ターゲットのレコードをグループメンバーテーブル 32 に追加する。ここで、追加される iSCSI イニシエータのレコードのエントリ 320 には領域 421 の内容、エントリ 321 にはエントリ 332 に登録された IP アドレス、エントリ 322 には「イニシエータ」、エントリ 323 には「0」が登録される。又、追加される iSCSI ターゲットのレコードのエントリ 320 には領域 421 の内容、エントリ 321 にはエントリ 330 の iSCSI ネーム、エントリ 322 には「ターゲット」、エントリ 323 には「0」が登録される。

#### 【0050】

図 5 は、システム管理者等が計算機システムに存在するスイッチの管理用ポートを登録するスイッチ登録画面 440 の表示例を示す図である。スイッチ登録画面 440 は、スイッチ ID を入力する領域 441、そのスイッチの管理用ポートの IP アドレスを入力する領域 442、これらの領域やボタンで指定された情報を登録する際に使用されるボタン 443、及び登録を取り消す際に使用されるボタン 444 を有する。

**【0051】**

以下、システム管理者等がGUIを用いてスイッチを登録する際の、ストレージ管理装置1の処理について説明する。

システム管理者等がポインティングデバイス等を用いてボタン443を指定すると、ストレージ管理装置1は、これらの領域やボタンで指定されたパラメータに基づき、スイッチテーブル35に新規レコードを追加する。

**【0052】**

次に、本実施形態における各装置間の通信シーケンスについて説明する。なお、ストレージ管理装置1とスイッチ3aとを接続する通信線20aは、デフォルトのVLANであるVLAN IDが0のVLANに属するように設定されているとする。さらに、他のスイッチ3が接続されたスイッチ3の物理ポートにはVLANトランクの設定をしておくものとする。

**【0053】**

図6(a)は、ストレージ装置2の物理ポートがスイッチ3に接続された時の例として、ストレージ装置2の物理ポート41が、スイッチ3aの物理ポート42に接続された時の双方の装置間での通信シーケンス例を示す図である。

まず、ストレージ装置2がリンク確立を検出すると、ストレージ装置2は、ディスクバリサービスに対してiSCSIターゲットを登録する。ディスクバリサービスとは、iSCSIイニシエータが利用可能なiSCSIターゲットのリストを取得するためのサービスであり、IETFではSLP(Service Location Protocol、RFC2608)やiSNS(Internet Simple Name Service)を使った実装が提案されている。

**【0054】**

本実施形態では、ストレージ管理装置1がSLPのディレクトリエージェントとして動作するものとする。なお、iSNSを使用する場合にも本発明は適用可能である。SLPが用いられる場合、iSCSIターゲットの登録は、サービス広告パケットの送信によって行われる。このサービス広告パケットには、iSCSIターゲットのiSCSIネーム、IPアドレス、及びポート番号などが含ま

れる。なお、この時点で、物理ポート 4 1 と物理ポート 4 2 を接続する通信線 2 0 a は、デフォルトの V L A N ( V L A N I D = 0 ) に属する ( S 6 0 1 ) 。

#### 【0055】

i S C S I ターゲットからサービス広告を受信したストレージ管理装置 1 は、そのサービス広告の内容に基づき i S C S I ネームテーブル 3 4 にレコードを追加した後、アドレステーブル更新処理を実行する ( S 6 0 2 から S 6 0 5 ) 。

具体的には、ストレージ管理装置 1 はまず、通信線 2 0 a 経由で A R P 要求をブロードキャスト送信する。この時点で、ストレージ管理装置 1 とスイッチ 3 a とを接続する通信線 2 0 a と物理ポート 4 1 と物理ポート 4 2 とを接続する通信線 2 0 a は同一の V L A N に属しているため、このブロードキャストパケットは物理ポート 4 1 に到達する ( S 6 0 2 ) 。

#### 【0056】

ブロードキャストパケットを受信したストレージ装置 2 は、物理ポート 4 1 の M A C アドレスを含む A R P 応答をストレージ管理装置 1 に送信する。これにより、ストレージ管理装置 1 が i S C S I ターゲットの I P アドレスに対応する M A C アドレスを得る ( S 6 0 3 ) 。

次に、ストレージ管理装置 1 は、スイッチ 3 a から通信線 2 0 b 経由でフォーワーディングデータベースを取り出し、M A C アドレスに対応するポート I D (物理ポート 4 2 のポート I D) を得る。

#### 【0057】

その後、ストレージ管理装置 1 は、上述のようにして得られた物理ポート 4 1 の I P アドレス、M A C アドレス及び接続先物理ポート 4 2 のポート I D との対応関係をアドレステーブル 3 0 に記憶する ( S 6 0 4 、 S 6 0 5 ) 。

#### 【0058】

最後に、ストレージ管理装置 1 は、V L A N 追加処理を実行する。この V L A N 追加処理では、ストレージ管理装置 1 はまず、S 6 0 1 で受信したサービス広告パケットに含まれていた i S C S I ターゲットの i S C S I ネームをキーにグループメンバテーブル 3 2 を検索し、i S C S I ターゲットが属するグループのグループ I D を得る。そして、このグループ I D を V L A N I D として持つ V

L A Nに物理ポート 4 2 が属するように、ストレージ管理装置 1 は、通信線 2 0 b 経由でスイッチ 3 a に対して V L A N の設定の指示を行う ( S 6 0 6、S 6 0 7 )。

#### 【 0 0 5 9 】

図 6 ( b ) は、ホスト 4 がスイッチ 3 に接続された時の例として、ホスト 4 a がスイッチ 3 a に接続された時の通信シーケンス例を示す図である。

尚、本通信シーケンスは、最初にホスト 4 a がストレージ管理装置 1 に対して利用可能な i S C S I ターゲットを取得するためのサービス要求を送信すること ( S 6 1 1 ) と、最後にストレージ管理装置 1 が、通信線 2 0 a 経由でホスト a に利用可能な i S C S I ターゲットを送信すること ( S 6 1 8 ) 以外のステップは、図 6 ( a ) と同様である。また、ホスト 4 c 又は 4 d がスイッチ 3 b に接続された時の通信シーケンスは、ホスト 4 とスイッチ 3 a の間にスイッチ 3 b が入る以外、図 6 ( a ) と同様である。

#### 【 0 0 6 0 】

図 6 ( c ) は、ストレージ装置 2 の物理ポート又はホスト 4 の物理ポートがスイッチから切断された時の例として、ホスト 4 a がスイッチ 3 a から切断された時の通信シーケンス例を示す図である。

ホスト 4 a とのリンクの切断を検出したスイッチ 3 a は、S N M P T r a p などの手段を用いて、通信線 2 0 b 経由でストレージ管理装置 1 にリンクダウン通知を送信する。このリンクダウン通知にはリンクダウンした物理ポートのポート I D が含まれているものとする ( S 6 2 1 )。

#### 【 0 0 6 1 】

リンクダウン通知を受信したストレージ管理装置 1 は、そのリンクダウン通知からポート I D とソース I P アドレス (送信元のスイッチの I P アドレス) の情報を取り出す。そして、ストレージ管理装置 1 は、ソース I P アドレスをキーにスイッチテーブル 3 5 を検索し、合致したレコードからスイッチ I D を取り出す。更にストレージ管理装置 1 は、取り出したポート I D とスイッチ I D との組をキーにアドレステーブル 3 0 を検索し、合致したレコードの I P アドレスを後述の V L A N 削除処理で使うために主メモリ 2 1 の任意の領域に待避した上で、そ



のレコードを削除する (S 6 2 2)。

#### 【0062】

最後に、ストレージ管理装置 1 は、VLAN 削除処理を実行する。この VLAN 削除処理では、ストレージ管理装置 1 は、リンクが切断されたホスト 4、或いはストレージ装置 2 の物理ポートを VLAN から削除する VLAN 設定要求を、スイッチ 3 a に通信線 20 b 経由で送信する (S 6 2 3、S 6 2 4)。

#### 【0063】

次に、図 6 で説明したアドレステーブル更新処理、VLAN 追加処理及び VLAN 削除処理の詳細な処理手順について説明する。

#### 【0064】

図 7 は、ストレージ管理装置 1 におけるアドレステーブル取得処理の動作手順を示すフローチャートである。

サービス広告パケット又はサービス要求パケットを受信したストレージ管理装置 1 は、サービス要求受信プログラム 11 を実行して、受信したサービス広告パケット、或いはサービス要求パケットからパケット送信元の IP アドレスを取り出す (S 7 0 1)。

#### 【0065】

次に、ストレージ管理装置 1 は、ARP 送信プログラム 12 を実行して、S 7 0 1 で得た IP アドレスの MAC アドレスを問い合わせるための ARP 要求を組み立て、通信線 20 a にブロードキャスト送信する (S 7 0 2)。S 7 0 2 の ARP 要求に対応する ARP 応答を受信したストレージ管理装置 1 は、ARP 送信プログラム 12 を実行して、その ARP 応答から MAC アドレスを取り出す (S 7 0 3)。

#### 【0066】

次に、ストレージ管理装置 1 は、ポート ID 取得プログラム 13 を実行して、スイッチテーブル 35 の先頭レコードを取り出し (S 7 0 4)、当該レコードの管理用 IP アドレス宛てに、フォワーディングデータベースの取得要求を通信線 20 b 経由で送信する。このフォワーディングデータベースの取得要求は、例えば、SNMP (Simple Network Management Pro

protocol) Getを用いて、MIB-2 (Management Information Base-2、RFC1213) のipNetToMedia Tableを取得することにより実現できる (S705)。

#### 【0067】

その後、ストレージ管理装置1は、取得したフォワーディングデータベースを、S703で得たMACアドレスをキーに検索する (S706)。検索の結果該当するエントリが存在したら (S707)、ストレージ管理装置1は、S701で得たIPアドレス、S703で得たMACアドレス、S704で取り出したレコードのスイッチID、及びS707で得たエントリのポートIDを用いて、アドレステーブル30に新規レコードを追加する (S708)。

#### 【0068】

もし、S707で該当するエントリが存在しなかったら、ストレージ管理装置1は、スイッチテーブル35の全てのレコードに関してS705からS707を繰り返す (S709、S710)。

#### 【0069】

図8は、ストレージ管理装置1で行われるVLAN追加処理の動作を示すフローチャートである。

最初に、ストレージ管理装置1は、VLAN設定プログラム15を実行して、図7のS701で受信したサービス広告パケット、或いはサービス要求パケットから、それぞれiSCSIターゲットのiSCSIネーム、或いはiSCSIイニシエータのIPアドレスを取り出す (S801)。

#### 【0070】

そして、ストレージ管理装置1は、S801で取り出したiSCSIネーム、或いはIPアドレスをキーにグループメンバテーブル32を検索し、グループIDを得る (S802)。

次に、ストレージ管理装置1は、S802で得たグループIDをキーにグループメンバテーブル32を再度検索する (S803)。その結果、グループIDを検索する際にキーとしたiSCSIターゲット或いはiSCSIイニシエータがグループ内の最初のiSCSIノードである場合、すなわち、S803の検索で

得た全てのレコードのエントリ 323 の接続フラグの値が 0 の場合 (S804)、ストレージ管理装置 1 は、S802 で得たグループ ID を VLAN ID として持つ VLAN の作成要求を通信線 20b 経由でスイッチへ送信する (S805)。

#### 【0071】

S805 の処理の終了後又は S804 でいずれかのレコードのエントリ 323 の値が 1 であった場合、ストレージ管理装置 1 は、作成された (あるいは既存の) VLAN へ、図 7 の S707 で得たポート ID を追加する VLAN 追加要求を通信線 20b 経由で送信する。尚、この VLAN 作成要求及び VLAN 追加要求の宛先は、図 7 の S704、或いは S710 で取り出したレコードの管理用 IP アドレス 351 である (S806)。

#### 【0072】

その後、必要であれば、ストレージ管理装置 1 は、スイッチの設定を保存、有効化するパケットをスイッチ 3 へ送信してもよい。最後に、ストレージ管理装置 1 は、S802 の検索条件に合致したレコードのエントリ 323 の値を 1 に変更する (S807)。

#### 【0073】

図 9 は、ストレージ管理装置 1 における VLAN 削除処理の動作を示すフローチャートである。

最初に、ストレージ管理装置 1 は、VLAN 設定プログラム 15 を実行して、図 6 (c) の S622 で待避した IP アドレスをキーに iSCSI ネームテーブル 34 を検索する (S901)。S901 の検索でレコードが見つかった場合 (S902)、ストレージ管理装置 1 は、通信線 20 から切断されたのは iSCSI ターゲットと判断し、当該レコードの iSCSI ネーム 340 を取り出し、その iSCSI ネームをキーにグループメンバテーブル 32 を検索する (S903)。

#### 【0074】

一方、S901 の検索でレコードが見つからなかった場合 (S902)、ストレージ管理装置 1 は、通信線 20 から切断されたのは iSCSI イニシエータと

判断し、検索に使用した IP アドレスをキーにグループメンバテーブル 32 を検索する (S904)。

#### 【0075】

S903 又は S904 の検索でレコードが見つからなかった場合 (S905)、ストレージ管理装置 1 は処理を終了する。一方、S905 でレコードが見つかった場合、ストレージ管理装置 1 は、発見されたレコードからグループ ID を取り出す。そして、ストレージ管理装置 1 は、取り出したグループ ID を VLAN ID として持つ VLAN から図 6 (c) の S621 のリンクダウン通知に含まれていたポート ID を削除する VLAN 解除要求を、通信線 20b 経由でスイッチに送信する (S906)。

#### 【0076】

そして、ストレージ管理装置 1 は、S903 又は S904 の検索で見つかったレコードのエントリ 323 を 0 に変更する (S907)。

次に、ストレージ管理装置 1 は、先の処理で取り出したグループ ID をキーにグループメンバテーブル 32 を再検索する (S908)。その結果、当該 iSCSI ターゲット又は iSCSI イニシエータがグループ内の最後の iSCSI ノードである場合、すなわち、S908 の検索で得た全てのレコードの接続フラグ 323 が 0 の場合のみ (S909)、ストレージ管理装置 1 は、グループ ID に対応する VLAN の削除要求をネットワーク 20b 経由でスイッチへ送信する (S910)。

#### 【0077】

その後、必要であれば、ストレージ管理装置 1 は、スイッチの設定を保存、有効化するパケットをスイッチ 3 に送信してもよい。なお、S906 の VLAN 解除要求及び S910 の VLAN 削除要求の宛先は、図 6 (c) の S622 で得たスイッチテーブル 35 のレコードの管理用 IP アドレス 351 である。

#### 【0078】

以上で説明した第一の実施形態によると、システム管理者が、LUN マスキング設定と共に、グループを構成するホスト 4 やストレージ装置 2 が属する VLAN のサブネットアドレスの入力を行うだけで、ホスト 4 やストレージ装置 2 がネ

ネットワークに接続された時に、ストレージ管理装置 1 が、自動的に VLAN の設定の指示を行う。これにより、システム管理者は、IP-SAN のセキュリティ対策に伴う運用負荷を大幅に軽減することが可能となる。

#### 【0079】

次に、第二の実施形態について説明する。但し、第一の実施形態と相違する部分に限って説明する。第二の実施形態では、上述した IP-SAN セキュリティ管理が、スイッチ 3' で実施される。

#### 【0080】

図 10 は、ストレージ装置 2、スイッチ 3' a、3 b、ホスト 4 a、4 b、4 c 及び 4 d が通信線 20 a を介して相互に接続されている計算機システムの構成を示す図である。ストレージ装置 2、スイッチ 3' a 及びスイッチ 3 b は、管理用のデータが流れる通信線 20 b によっても相互に接続されている。以下、スイッチ 3' a で IP-SAN セキュリティ管理方法が実施されるものとする。

#### 【0081】

スイッチ 3' a は、ネットワークからのデータ受信、ネットワーク又はデータ転送部 51 へのデータ送信を行うデータ送受信部 50、二つのデータ送受信部 50 の間でデータを転送するバス又はクロスバースイッチであるデータ転送部 51、フォワーディングデータベース格納部 52、フォワーディングデータベース格納部 52 の内容に基づきデータ送受信部 50 のデータ送信先を制御するデータ転送制御部 53、GUI 制御部 10'、ディスクバリ要求受信部 11'、ARP 送信部 12'、ポート ID 取得部 13'、LUN マスキング設定部 14'、VLAN 設定部 15' 及び主メモリ 21 を有する。

#### 【0082】

なお、本実施形態では、スイッチ 3' a が二つのデータ送受信部 50 を備えるものとしているが、一つ、或いは三つ以上のデータ送受信部 50 を備えてもよい。又、本実施形態では、GUI 制御部 10' 等をハードウェアとして実現しているが、第一の実施形態と同様に主メモリ 21 に格納されたソフトウェアプログラムとしてその機能を実現しても良い。

又、スイッチへの設定情報の入力、管理用ネットワークを介して管理端末か

ら行う。

#### 【0083】

主メモリには、アドレステーブル30、グループテーブル31、グループメンバーテーブル32、LUNマスキングテーブル33、iSCSIネームテーブル34及びスイッチテーブル35が格納される。スイッチテーブル35には、スイッチ3'a以外のスイッチ3の管理用IPアドレスが登録される。

#### 【0084】

次に、第二の実施形態における通信シーケンスについて説明する。

図11は、ホスト4aがスイッチ3'aに接続された時の通信シーケンス例を示す図である。

ホスト4aがスイッチ3'aに接続された後、ホスト4aはまず、サービス要求をスイッチ3aに送信する(S1101)。そのサービス要求を受信したスイッチ3'aは、ARP送信部12を用いてホスト4aにARP要求を送信して、ホスト4aのMACアドレスを得る(S1102, S1103)。

#### 【0085】

次にスイッチ3'aは、データ転送制御部53を用いて、フォワーディングデータベース格納部52からフォワーディングデータベースの内容を読み出す。更に、スイッチ3'aのポートID取得部13は、このようにして得たフォワーディングデータベースをS1103で得たMACアドレスをキーに検索する。MACアドレスに対応するエントリが見つかった場合、スイッチ3'aは、ホスト4aが自身に直接(他のスイッチを介さずに)接続されている装置であると判断し、検索されたエントリからポートIDを得る(S1104)。

#### 【0086】

そして、VLAN設定部15が、前記サービス要求の送信元IPアドレスをキーにグループテーブル31を検索し、その結果得たレコードのグループID310を取り出す。さらに、データ転送制御部53に対して、前記グループIDをVLAN IDに持つVLANに、S1104で得たポートIDを追加するVLAN設定を要求する。その後、データ転送制御部53は、受信したVLAN設定の内容をデータ送受信部50に通知し、データ送受信部50がVLANの処理がで

きるようになる (S1105)。最後に、スイッチ 3' a のディスカバリ要求受信部 11 は、ホスト 4 a にサービス応答を返信する (S1106)。

#### 【0087】

なお、S1104 でエントリが見つからなかった場合、スイッチ 3' a は、第一の実施形態と同様の処理を行う。例えば、ホスト 4 c がスイッチ 3 b と接続された時の通信シーケンスは、ホスト 4 a がホスト 4 c である点、スイッチ 3 a がスイッチ 3 b である点及びストレージ管理装置 1 がスイッチ 3' a である点を除き、図 6 (b) と同様である。

#### 【0088】

次に、第三の実施形態を説明する。本実施形態では、上述した IP-SAN セキュリティ管理を、ストレージ装置 2 が実施する。本実施形態では、ストレージ装置 2 は、主メモリ 21 と磁気ディスク 23 を備える。主メモリ 21 に GUI 制御プログラム 10、ディスカバリ要求受信プログラム 11、ARP 送信プログラム 12、ポート ID 取得プログラム 13、LUN マスキング設定プログラム 14 及び VLAN 設定プログラム 15 が格納される。磁気ディスク 23 に、アドレステーブル 30、グループテーブル 31、グループメンバテーブル 32、LUN マスキングテーブル 33、iSCSI ネームテーブル 34 及びスイッチテーブル 35 が格納される。本実施形態の動作手順は、ストレージ管理装置 1 がストレージ装置 2 に変更される以外は、第一の実施形態と同様である。

#### 【0089】

##### 【発明の効果】

本発明により、IP-SAN における LUN マスキングと VLAN の設定を一元化できるため、システム管理者の設定作業負荷が軽減され、かつミス発生率も低減できる。結果として、IP-SAN の運用コストを削減可能である。

##### 【図面の簡単な説明】

##### 【図 1】

第一の実施形態におけるシステム構成例を示す図である。

##### 【図 2】

各テーブルのデータ構造例を示す図である。

**【図 3】**

各テーブルのデータ構造例を示す図である。

**【図 4】**

グループ登録画面の表示例を示す図である。

**【図 5】**

L U N マスキング設定画面、スイッチ登録画面の表示例を示す図である。

**【図 6】**

第一の実施形態における通信シーケンス例を示す図である。

**【図 7】**

アドレステーブル更新処理の動作を示すフローチャートである。

**【図 8】**

V L A N 追加処理の動作を示すフローチャートである。

**【図 9】**

V L A N 削除処理の動作を示すフローチャートである。

**【図 1 0】**

第二の実施形態のシステム構成例を示す図である。

**【図 1 1】**

第二の実施形態における通信シーケンス例を示す図である。

**【符号の説明】**

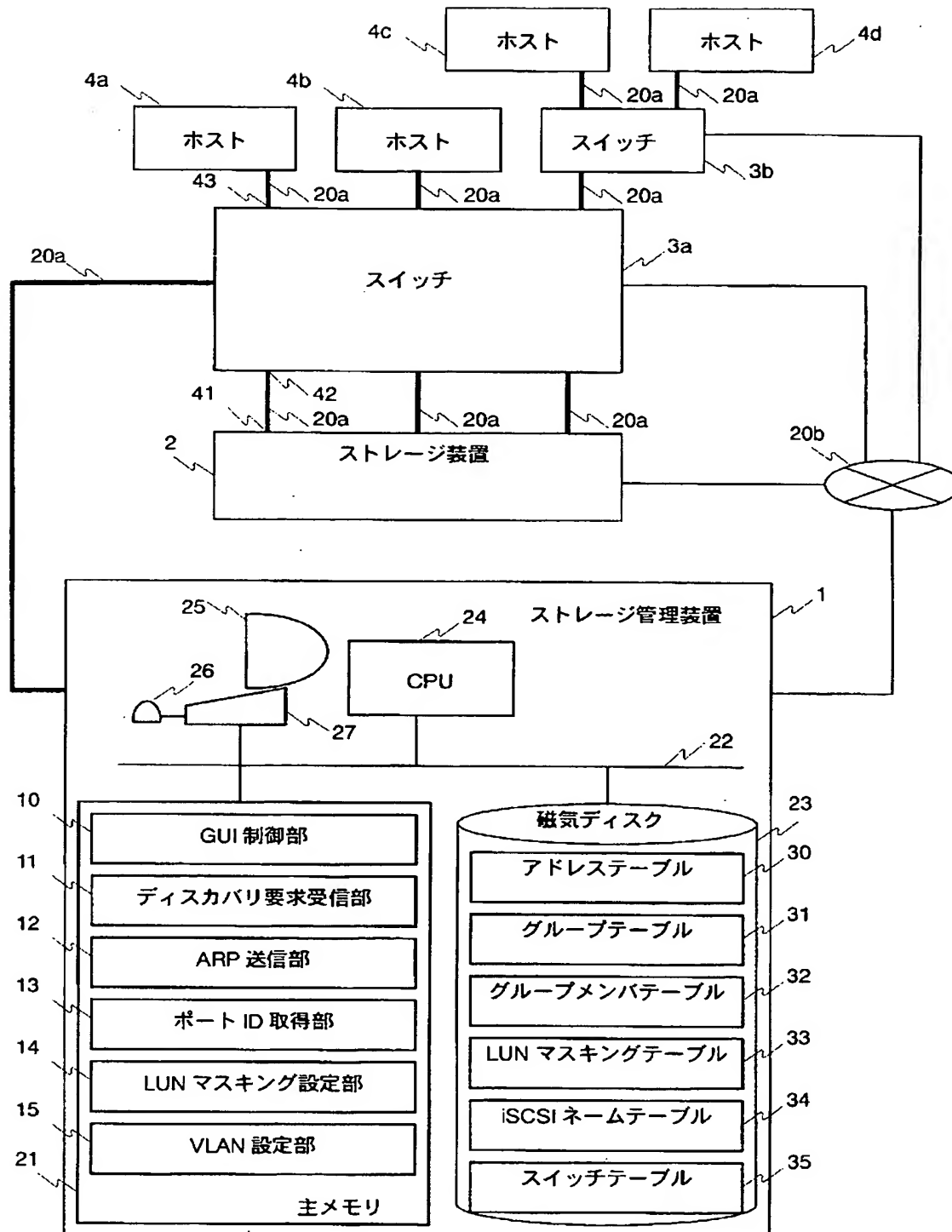
1…ストレージ管理装置、2…ストレージ装置、3…スイッチ、4…ホスト、20…通信線、21…主メモリ、22…通信線、23…磁気ディスク、24…CPU、25…ディスプレイ、26…ポインティング装置、27…文字入力装置、41、42、43…物理ポート。



【書類名】 図面

【図 1】

図 1



【図 2】

図 2

(a) アドレステーブル 30

300 IP アドレス	301 MAC アドレス	302 スイッチ ID	303 ポート ID
192.168.1.1	11-22-33-44-55-01	3a	1
192.168.2.1	11-22-33-44-55-02	3a	2
192.168.1.2	11-22-33-44-55-03	3b	1
192.168.2.2	11-22-33-44-55-04	3b	2
...	...	...	...

(b) グループテーブル 31

310 グループ ID	311 サブネットアドレス
1	192.168.1.0/24
2	192.168.2.0/24
...	...

(c) グループメンバテーブル 32

320 グループ ID	321 アドレス	322 種別	323 接続フラグ
1	iqn.2000-02.com.hitachi:users:test1	ターゲット	1
1	192.168.1.1	イニシエータ	1
1	192.168.1.2	イニシエータ	0
2	192.168.2.1	イニシエータ	0
...	...	...	...

【図 3】

図 3

(a) LUN マスキングテーブル 33

iSCSI ネーム	LUN	IP アドレス
iqn.2000-02.com.hitachi:users:test1	1	192.168.1.1
iqn.2000-02.com.hitachi:users:test1	1	192.168.1.2
...	...	...

(b) iSCSI ネームテーブル 34

iSCSI ネーム	IP アドレス	ポート番号
iqn.2000-02.com.hitachi:users:test1	192.168.1.254	3260
iqn.2000-02.com.hitachi:users:test2	192.168.2.254	3260
...	...	...

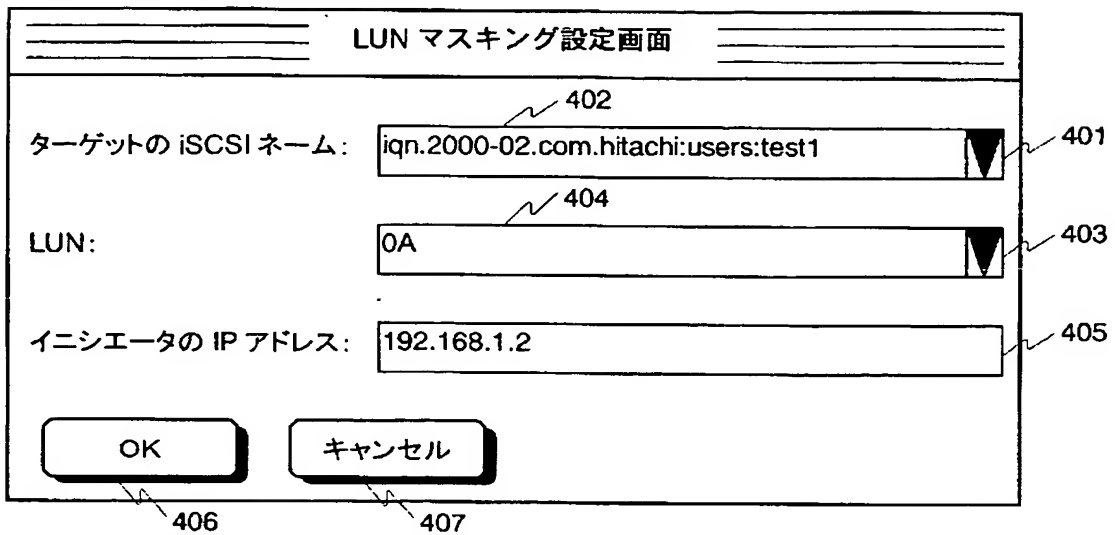
(c) スイッチテーブル 35

スイッチ ID	管理用 IP アドレス
3a	192.168.0.1
3b	192.168.0.2
...	...

【図 4】

図 4

(a) LUN マスキング設定画面 400



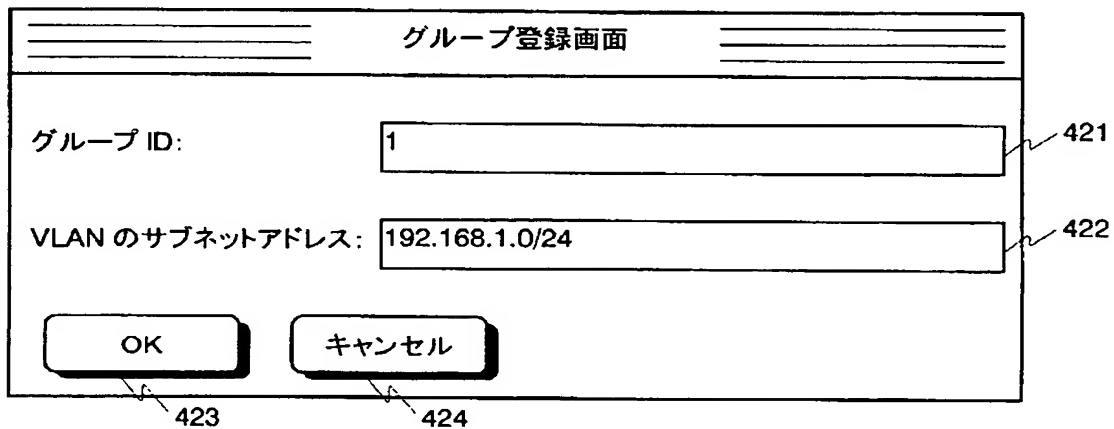
The diagram shows a window titled "LUN マスキング設定画面" (LUN Masking Setting Screen). It contains three input fields: "ターゲットの iSCSI ネーム:" (Target iSCSI Name) with value "iqn.2000-02.com.hitachi:users:test1", "LUN:" with value "0A", and "イニシエータの IP アドレス:" (Initiator IP Address) with value "192.168.1.2". At the bottom are "OK" and "キャンセル" (Cancel) buttons.

ターゲットの iSCSI ネーム:

LUN:

イニシエータの IP アドレス:

(b) グループ登録画面 420



The diagram shows a window titled "グループ登録画面" (Group Registration Screen). It contains two input fields: "グループ ID:" (Group ID) with value "1" and "VLAN のサブネットアドレス:" (VLAN Subnet Address) with value "192.168.1.0/24". At the bottom are "OK" and "キャンセル" (Cancel) buttons.

グループ ID:

VLAN のサブネットアドレス:

【図 5】

図 5

(a) スイッチ登録画面 440

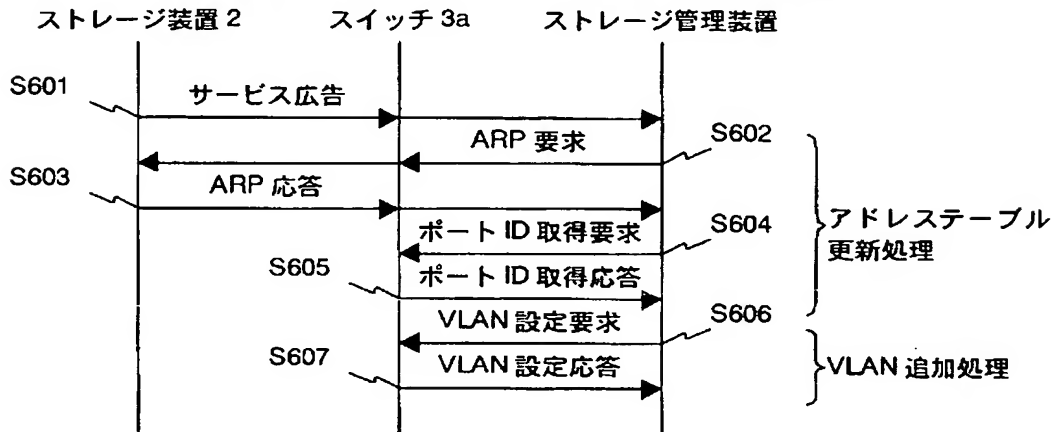
The diagram shows a rectangular window titled "スイッチ登録画面" (Switch Registration Screen). Inside the window, there are two input fields. The first field is labeled "スイッチID:" (Switch ID:) and contains the value "1". The second field is labeled "管理用ポートの IP アドレス:" (Management Port IP Address:) and contains the value "192.168.0.2". Below these fields are two buttons: "OK" and "キャンセル" (Cancel). The labels 441, 442, 443, and 444 point to the first input field, the second input field, the OK button, and the Cancel button, respectively.

スイッチ登録画面	
スイッチID:	1
管理用ポートの IP アドレス:	192.168.0.2
OK	キャンセル

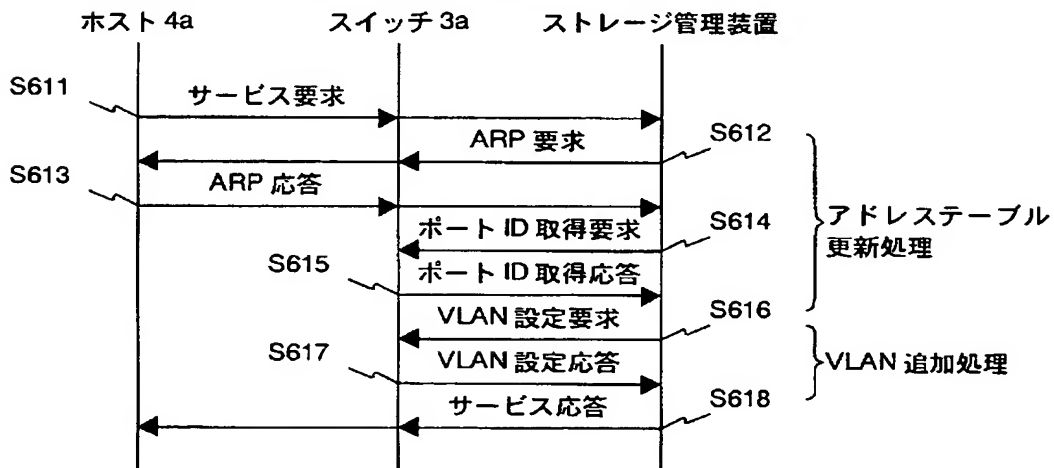
【図 6】

図 6

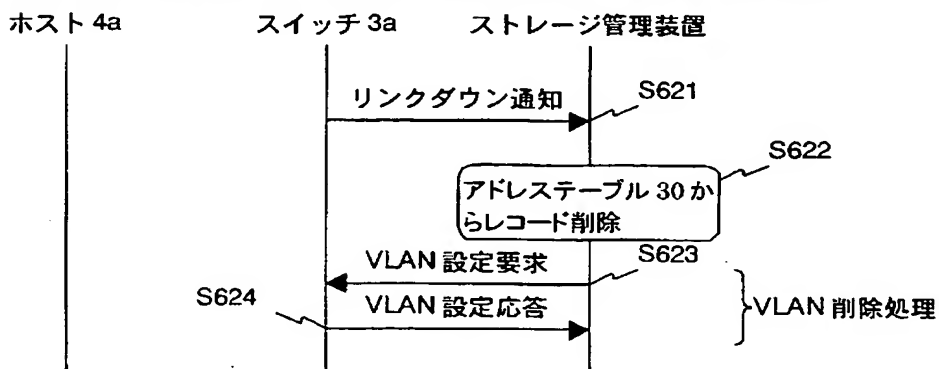
(a) ストレージ装置の物理ポートがスイッチに接続された時の通信シーケンス



(b) ホストがスイッチに接続された時の通信シーケンス

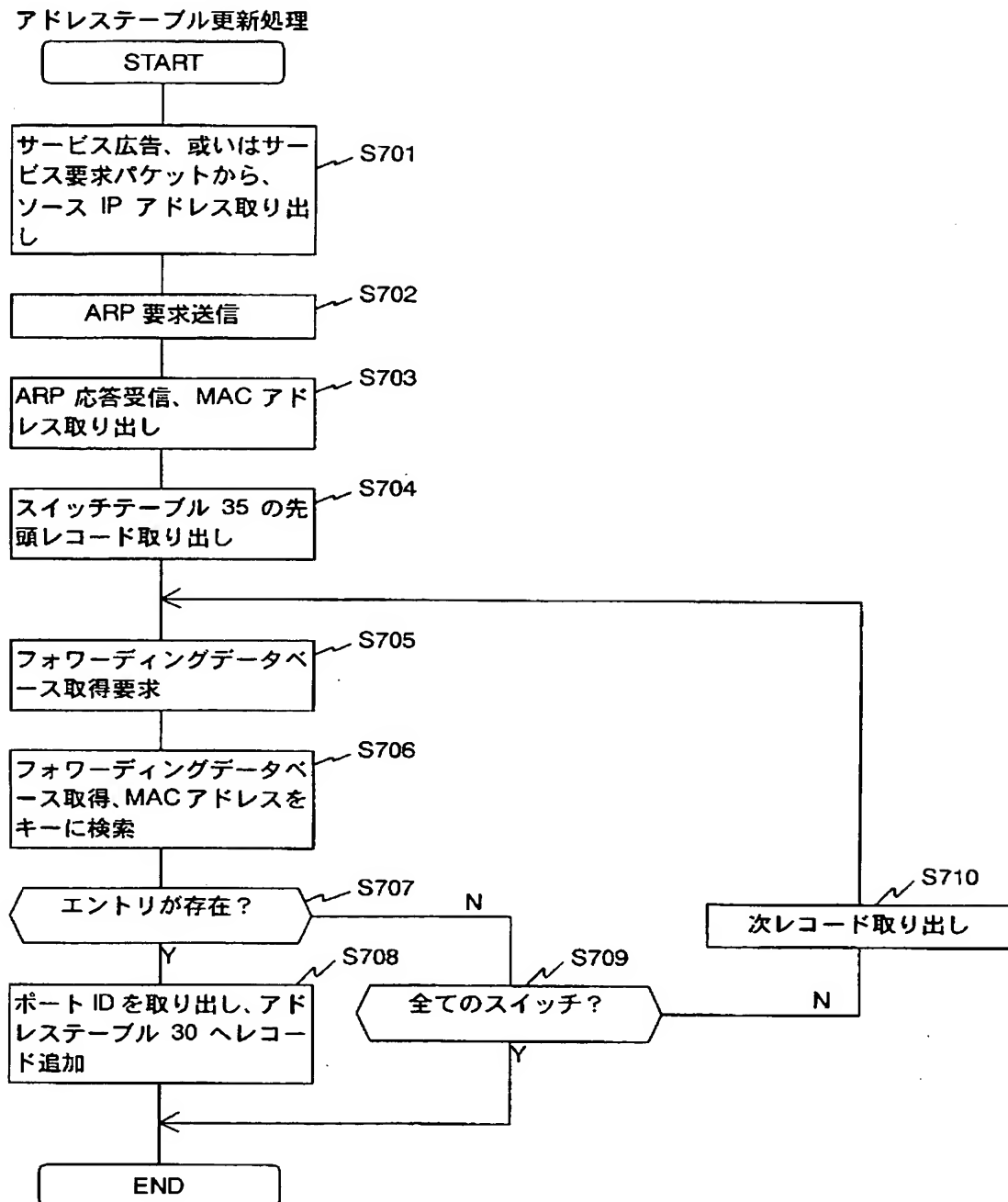


(c) ストレージの物理ポート、ホストがスイッチから切断された時の通信シーケンス



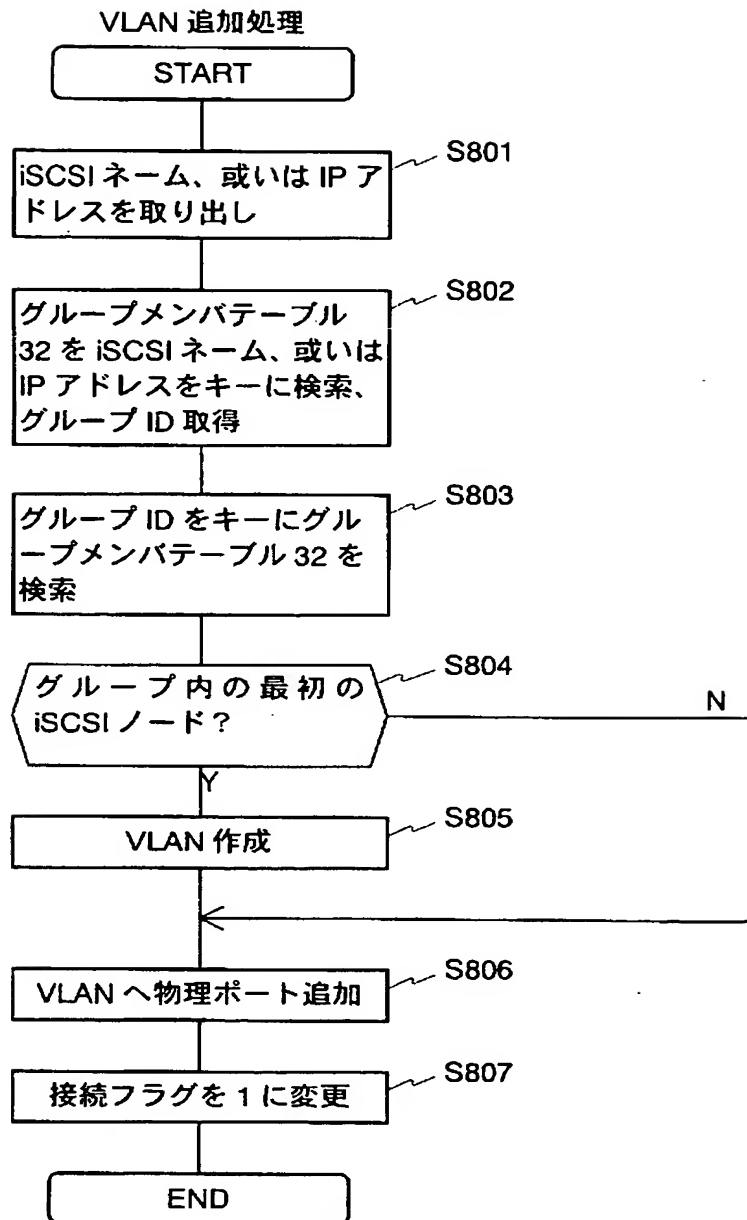
【図 7】

図 7



【図 8】

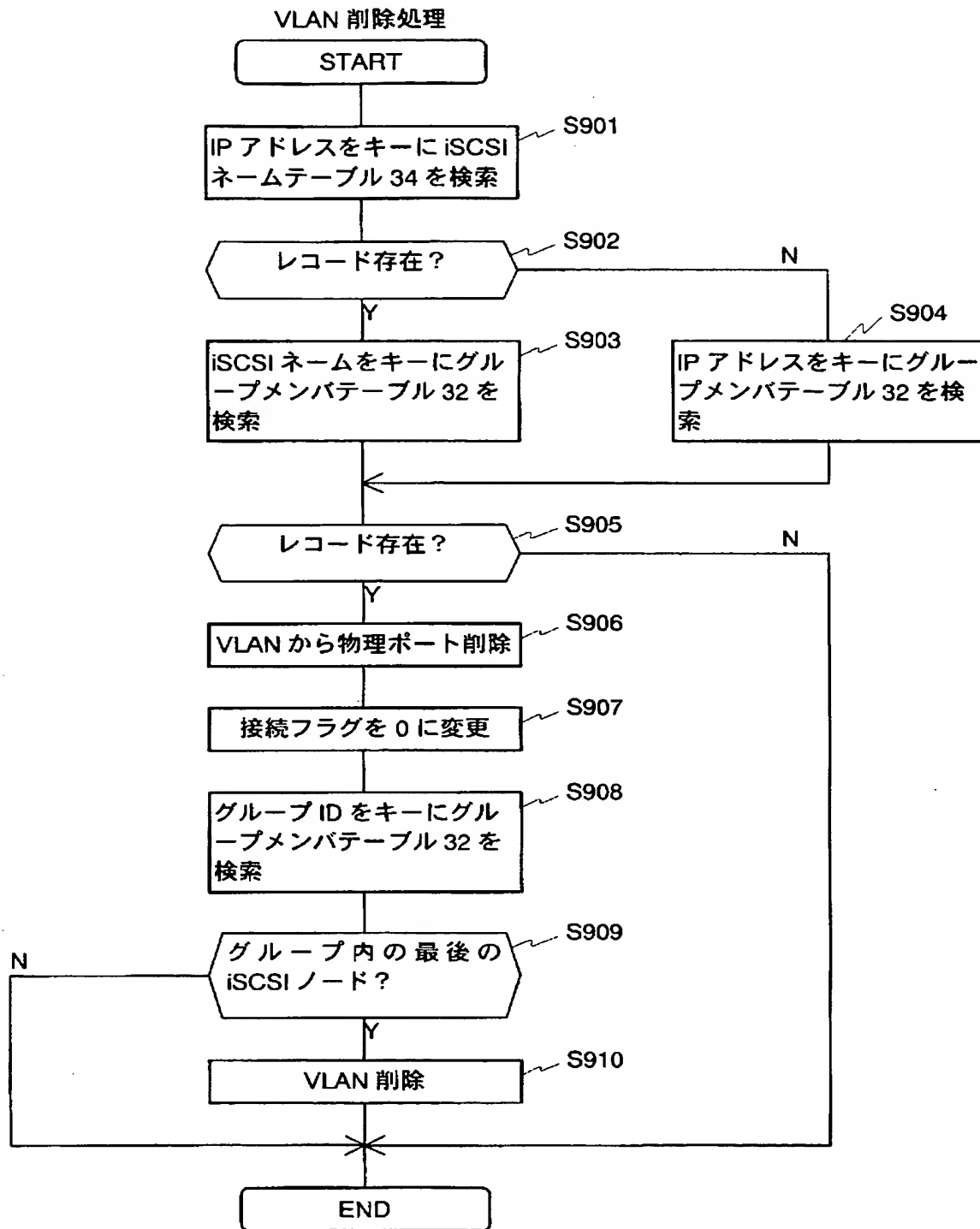
図 8





【図 9】

図 9

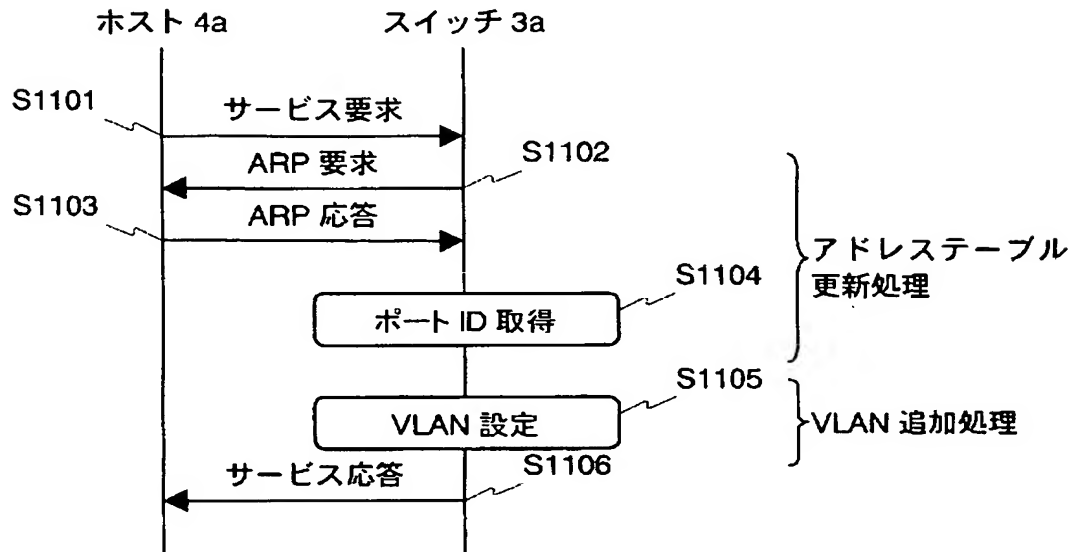




【図 11】

図 11

(a) ホスト 4a がスイッチ 3a に接続された時の通信シーケンス



【書類名】 要約書

【要約】

【課題】

I P-S A Nのセキュリティ対策にとって不可欠なL U NマスキングとV L A Nの設定を、システム管理者が一元管理できるようにすることで、I P-S A Nの運用コストを削減する。

【解決手段】

ストレージ装置、スイッチ及びホストがネットワークで接続されている計算機システムにおいて、ストレージ装置の論理ボリュームの識別子とホストのI Pアドレスに基づき、論理ボリュームに対するアクセス制御設定をストレージ装置に対して実行し、ホストのI PアドレスをM A Cアドレスに変換し、ホストのM A Cアドレスをホストが接続しているスイッチのポートI Dに変換し、ポートをV L A Nに追加する設定をスイッチに対して実行する。

【選択図】 図1

認定・付加情報

特許出願の番号	特願 2003-206165
受付番号	50301300017
書類名	特許願
担当官	第八担当上席 0097
作成日	平成15年 8月 7日

<認定情報・付加情報>

【提出日】 平成15年 8月 6日

特願 2 0 0 3 - 2 0 6 1 6 5

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 5 1 0 8 ]

1. 変更年月日

1 9 9 0 年 8 月 3 1 日

[変更理由]

新規登録

住 所

東京都千代田区神田駿河台 4 丁目 6 番地

氏 名

株式会社日立製作所